REMARKS/ARGUMENTS

Claim 98 is pending in this application. Claim 98 is hereby amended and new claims 99-109 are submitted for entry and examination. Thus, following this amendment, claims 98-109 will be pending.

In the Office Action, the Examiner again rejected claim 98 under 35 USC §103(a) as being unpatentable over Ganesan (U.S. Patent Number 5,535,276) (hereinafter referred to as "Ganesan"), in view of Johnson et al. (U.S. Patent Number 5,815,573) (hereinafter referred to as "Johnson") and Matyas et al. (U.S. Patent Number 5,142,578) (hereinafter referred to as "Matyas"). Reconsideration in view of the amendments made herein and the following remarks is respectfully requested.

Claim 98

Amended claim 98 recites, among other elements, "combining the most significant portion, without encryption, and the encrypted version of the least significant portion to form a storable private key sequence, the storable private key sequence being such that a decryption of the storable private key sequence using a proposed secret other than the secret known to the user results in a decrypted pseudo-key, wherein a pseudo-key is a key that conforms to the predetermined key format but does not match the private key and wherein the number of proposed secrets that lead to a pseudo-key is larger than a security threshold".

The specification shows a method for secure cryptographic key storage, in which a malicious hacker who exhaustively tries all possible PINs to recover a private key where the private key was encoded using a PIN that was the only correct PIN of all possible PINs. The hacker will recover one private key (which was encoded using the one valid PIN) and *many* pseudo-keys, each of which appears well-formed (i.e., compliant with a predetermined key format). As the hacker attempts to use the keys in an effort to determine which is the real private key, it is more likely that a security threshold number of attempts will be reached before a valid private key is detected.

One way to ensure that candidate private keys are well formed is to divide the (correct) private key d into a most significant portion and a least significant portion, d_a and d_b, where the concatenation of d_a and d_b equals d. The most significant portion is then combined with different least significant portions to form candidate private keys. This ensures that the magnitude of a candidate private key remains smaller than a modulus so that the candidate private key is well-formed.

Claim 104

New claim 104 recites, among other elements, "combining the first portion, without encryption, and the encrypted second portion to form a storable private key sequence, the storable private key sequence being such that a decryption of the storable private key sequence using at least some proposed secrets other than the secret known to the user results in a decrypted pseudo-key, wherein the number of proposed secrets that lead to a pseudo-key is larger than a security threshold".

The Cited References

Ganesan teaches splitting a user private key into two portions.

Johnson teaches a key recovery system that accommodates legitimate concerns of law enforcement officials while at the same time resists attacks by unauthorized parties. Two communicating users Alice and Bob agree upon a randomly generated secret value referred to as the PQR value, from which an encryption key is generated. The PQR value comprises an m-bit P value, an m-bit Q value and an n-bit R value (column 6, lines 54-58). The P value is stored with a first key recovery agent, the Q value is stored with a second key recovery agent, and the R value is kept as a shared secret between Alice and Bob (column 6, lines 61-66, Figure 1). Key recovery agents will reveal P and Q to law enforcement officials upon the presentation of sufficient credentials, who then only need to ascertain the R value using available cryptanalytic means (column 1, lines 64-66).

Matyas teaches a method for generating and distributing a key-encrypting key (KEK) using a public-key cryptographic system (column 4, lines 51-57). Matyas merely uses

public and private keys of the public-key cryptographic system, and does not teach a method for secure cryptographic key storage.

Cited References Distinguished

Applicant submits that at least one element of each independent claim (and by extension, one element of each dependent claim) is not disclosed or suggested by any of the cited references, taken alone or in combination.

Ganesan may show splitting a user private key into two portions, but it does not close or suggest combining portions wherein one portion is encrypted and combined with an unencrypted portion to form a storable private key sequence, the storable private key sequence being such that a decryption of the storable private key sequence using at least some proposed secrets other than the secret known to the user results in a decrypted pseudo-key, wherein the number of proposed secrets that lead to a pseudo-key is larger than a security threshold.

Johnson is related to key recovery and as such does not disclose or suggest claimed elements lacking in Ganesan. For example, Johnson does not show the claimed storable private key sequence having the claimed properties.

Applicant submits that it is clear that Matyas does not make add to the teachings of Ganesan and Johnson such that the claimed elements could be found by the combination.

Applicant submits, for at least the reasons stated above, that the cited references do not render claims 98-109 obvious or anticipated. Hence, Applicant submits that claims 98-109 are patentable over Ganesan, Johnson and Matyas.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

Dated: 4/4/05

Philip H. Albert
Reg. No. 35,819

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200 Fax: 415-576-0300
PHA:jtc
60460114 v1